CLAIMS

What is claimed is:

1. A load balancing SSL acceleration device, comprising:

a processor, memory and communications interface;

a TCP communications manager capable of interacting with a plurality of client devices and server devices simultaneously;

a secure communications manager;

an encryption and decryption engine instructing the processor to encrypt data from a secure communications session and direct it to said second communication session; and

a load balancing engine associating ones of said client devices with ones of said servers for a communications session based on calculated processing loads of each said server.

2. The device of claim 1 wherein the TCP communications manager provides an IP address of an enterprise to said communications manager, and each of said plurality of servers is associated with the enterprise.

3. The device of claim 2 wherein the secure communications manager negotiates a secure communications session with each of said plurality of client devices over an open network.

4. The device of claim 3 wherein the TCP communications manager negotiates a separate, open communications session with one of the plurality of servers associated with the enterprise for each secure communications session negotiated with a client device.

5. The device of claim 4 wherein the encryption and encryption engine decrypts packet data received on the communications interface via a secure communications session, decrypts application data in the packet data and maps the data to an appropriate TCP session.

6. The device of claim 5 wherein the appropriate TCP session is selected by the load-balancing engine.

7. The device of claim 2 wherein the TCP communications manager responds to TCP communications negotiations directly for the enterprise.

8. The device of claim 2 wherein the TCP communications manager changes a destination IP address for each packet to a server for each session.

9. The device of claim 8 therein the secure communications engine negotiates a secure communication session for each TCP communications session.

10. The device of claim 9 wherein the secure communications manager responds to all secure communications with each client device.

11. The device of claim 9 wherein the secure communications manager changes a destination IP address fore each packet to a server IP address for each session.

12. A method for performing SSL acceleration of data communications between a plurality of customer devices attempting to communicate with an enterprise having a plurality of servers, comprising:

providing a device enabled for secure communication with customer devices and having an IP address associated with the enterprise;

receiving communications directed to the enterprise in a secure protocol from the customer devices;

decrypting data packets of the secure protocol to provide decrypted packet data;

selecting at least one of the plurality of servers in the enterprise based on a load calculation including processing sessions of other servers in the enterprise and associating the selected server with a communications session from one ; and

forwarding the decrypted packet data to the selected server of the enterprise.

13. The method of claim 12 further including the steps of:

receiving application data from the selected server of the enterprise;

encrypting the application data received from the selected server; and

forwarding encrypted application data to the customer device.

14. The method of claim 13 wherein the step of receiving secure communications directed to the enterprise includes receiving communications having a destination IP address of the enterprise.

15. The method of claim 14 further including the step of negotiating the secure protocol session with the customer device by responding as the enterprise to the customer devices.

16. The method of claim 14 further wherein the step of forwarding comprises:

modifying the destination IP address of data packets from the enterprise IP to an IP for the selected server.

17. The method of claim 14 wherein the step of forwarding comprises :

establishing an open communication session with the selected server, and

mapping the decrypted packet data to an open communications session established with the selected server.

18. The method of claim 17 wherein the open communications session is established via a secure network.

19. The method of claim 12 wherein the step of receiving comprises:

receiving SSL encrypted data having a length greater than a TCP segment carrying said data; and

wherein said step of decrypting comprises

buffering the SSL encrypted data in a memory buffer in the SSL accelerator device, the buffer having a length equivalent to the block cipher size necessary to perform the cipher; and

decrypting the buffered segment of the received SSL encrypted data to provide decrypted application data.

20. The method of claim 19 further including the step of authenticating the data on receipt of a final segment.

21. The method of claim 19 further including the step of generating an alert if said step of authenticating results in a failure.